# CWE Detail – CWE-473

## Description

A PHP application does not properly protect against the modification of variables from external sources, such as query parameters or cookies. This can expose the application to numerous weaknesses that would not exist otherwise.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Observed Examples (CVEs)

**•** CVE-2000-0860: File upload allows arbitrary file read by setting hidden form variables to match internal variable names.

**•** CVE-2001-0854: Mistakenly trusts $PHP\_SELF variable to determine if include script was called by its parent.

**•** CVE-2002-0764: PHP remote file inclusion by modified assumed-immutable variable.

**•** CVE-2001-1025: Modify key variable when calling scripts that don't load a library that initializes it.

**•** CVE-2003-0754: Authentication bypass by modifying array used for authentication.

## Related Attack Patterns (CAPEC)

* CAPEC-77

## Modes of Introduction

**•** Implementation: REALIZATION: This weakness is caused during implementation of an architectural security tactic.

## Common Consequences

**•** Impact: Modify Application Data — Notes:

## Potential Mitigations

**•** Requirements: Carefully identify which variables can be controlled or influenced by an external user, and consider adopting a naming convention to emphasize when externally modifiable variables are being used. An application should be reluctant to trust variables that have been initialized outside of its trust boundary. Ensure adequate checking is performed when relying on input from outside a trust boundary. Do not allow your application to run with register\_globals enabled. If you implement a register\_globals emulator, be extremely careful of variable extraction, dynamic evaluation, and similar issues, since weaknesses in your emulation could allow external variable modification to take place even without register\_globals. (Effectiveness: N/A)

## Applicable Platforms

**•** PHP (Class: None, Prevalence: Undetermined)

## Notes

**•** Relationship: This is a language-specific instance of Modification of Assumed-Immutable Data (MAID). This can be resultant from direct request (alternate path) issues. It can be primary to weaknesses such as PHP file inclusion, SQL injection, XSS, authentication bypass, and others.